Universität Bremen

IGMR
Institut für Informations-,
Gesundheits- und Medizinrecht

Universität Bremen | Postfach 33 04 40, 28334 Bremen
IGMR | FB06

Hessischer Landtag
Innenausschuss
Schlossplatz 1-3
65183 Wiesbaden

nachrichtlich per E-Mail

Bremen 26. April 2023

Fachbereich 06
Rechtswissenschaft

Prof. Dr. jur. Dennis-Kenji Kipker

GW 1
Universitätsallee
28359 Bremen

Tel. 0421 5905 5465
Fax 0421 218 66052
kipker@uni-bremen.de

www.igmr.uni-bremen.de
igmr@uni-bremen.de

Prof. Dr. jur. Dennis-Kenji Kipker

Schriftliche Stellungnahme

Gesetzentwurf der Landesregierung für ein Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG)

I. Vorbemerkung und rechtspolitischer Hintergrund

Eine Interpretation und Bewertung des vorliegenden Gesetzentwurfs muss vor dem Hintergrund der gesetzgeberischen und politischen Regelungsintention vorgenommen werden. Einerseits beschreibt das BSI in seinem Bericht zur Lage der IT-Sicherheit in Deutschland 2022 die Gefährdungslage als so hoch wie noch nie, andererseits nimmt die Nutzung und Vernetzung von IT rapide zu. So ergeben sich zwar die Bedarfe für die Digitalisierung, es wachsen jedoch auch die technischen Digitalisierungsrisiken gleichzeitig exponentiell an. Insbesondere die öffentliche Verwaltung steht unter einem zunehmenden Digitalisierungszwang, um die Erwartungen von Bürgerinnen und Bürgern an eine zeitgemäße und interessengerechte behördliche Infrastruktur zu erfüllen. Gleichzeitig wird von der Bevölkerung nicht nur erwartet, dass die digitalisierte Verwaltung im Sinne der Verfügbarkeit fehlerfrei funktioniert, sondern auch, dass (sensible) Bürgerdaten hinreichend vor unbefugter Offenlegung und Manipulation geschützt sind (Authentizität, Integrität und Vertraulichkeit). In diesem Spannungsverhältnis bewegt sich auch der vorliegende Gesetzentwurf, denn eine Gewähr für Cybersicherheit existiert nicht – umso wichtiger ist es daher auch, vor allem präventive Strukturen zu errichten.

Diese Aufgabe erfüllen soll auch das Hessen CyberCompetenceCenter (Hessen3C) im Zuständigkeitsbereich des Hessischen Ministeriums des Innern und für Sport, das als zentraler Ansprechpartner zum Thema Cybersicherheit in Hessen fungiert. Eingerichtet wurde Hessen3C im April 2019 innerhalb der Abteilung Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung und steht seither der hessischen Landesverwaltung, hessischen Kommunen und hessischen Unternehmen in beratender Funktion zur Verfügung. Hessen3C hat ein breit gefasstes Aufgabenspektrum, das nicht nur den Schutz der Landesverwaltung vor Cyberbedrohungen umfasst. Ebenso fällt in den Aufgabenbereich die Unterstützung der Sicherheitsbehörden bei der Ausbildung von Fachkräften, die Bekämpfung von Cybercrime und Cyberspionage sowie die Beratung von Kommunen, Wirtschaft und KRITIS. In letztgenanntem Zusammenhang ist Hessen3C zentra-

le Kontaktstelle zur Entgegennahme landesbezogener KRITIS-Meldungen. Aufgrund des weit gefassten Funktionszuschnitts besteht überdies eine enge Zusammenarbeit mit der Landespolizei und dem Landesamt für Verfassungsschutz. Folgende Leistungen erbringt Hessen3C konkret:

- **Leistungen für die Landesverwaltung:** Unterstützung und Koordinierung der Bearbeitung von Cybersicherheitsvorfällen in der Landesverwaltung. Zentrale Ansprechstelle bei IT-Sicherheitsvorfällen.
- **Leistungen für Kommunen:** Hessische Kommunen können die Leistungen des Hessen3C auf freiwilliger Basis und unter Wahrung des Selbstverwaltungsprinzips kostenfrei nutzen.
- **Leistungen für KRITIS:** Inanspruchnahme des Hessen3C durch KRITIS ist bei Bedarf kostenlos, ergebnisoffen und produktneutral möglich.
- **Leistungen für KMU:** Inanspruchnahme des Hessen3C durch KMU ist bei Bedarf kostenlos, ergebnisoffen und produktneutral möglich.

Mit dem Entwurf für ein HITSiG werden die umfangreichen Befugnisse des Hessen3C an eine Rechtsgrundlage angeknüpft, was gemessen am skizzierten Aufgaben- und Befugnisumfang sinnvoll, sachgerecht und juristisch notwendig erscheint – insbesondere auch deshalb, weil es bislang an einer umfassenden Rechtsgrundlage für Befugnisse und Datenzugriffe in Hessen fehlt, die jedoch dringend erforderlich ist, um Rechtssicherheit und Betroffenenschutz zu gewährleisten, da die Befugnisse teils Grundrechtsrelevanz besitzen. Überdies erfolgt die staatliche Gewährleistung der Cybersicherheit rechtlich nicht im „luftleeren Raum“ – vielmehr kann es zur Gewährleistung der Cybersecurity auch notwendig sein, andere und ebenfalls grundrechtlich geschützte Positionen inhaltlich zu verkürzen, sodass ein gesetzlich skizzierter Interessenausgleich sachgerecht ist. Ein behördliches Tätigwerden ohne entsprechende gesetzliche Grundlage wäre folglich nicht möglich bzw. rechtswidrig. Kernaspekte der zu treffenden Regulierung betreffen nachfolgende thematische Schwerpunkte:

- **Zentrum für Informationssicherheit:** U.a. Möglichkeit zum eigenständigen operativen Tätigwerden des Hessen3C in den Bereichen Prävention, Informationssammlung und -auswertung, Erarbeitung von Warnungen und Empfehlungen für Behörden und Öffentlichkeit, aktive Abwehr von Cybergefahren, Dienstleistungen/Auftragsverarbeitung für Kommunen, Einbindung des CERT.
- **Eingriffs- und Abwehrmaßnahmen:** U.a. Befugnis zur Datenanalyse zu Zwecken der Abwehr von Gefahren für die Cybersicherheit, insb. unter Einbeziehung personenbezogener Daten. Des Weiteren Möglichkeiten zur Untersuchung von im Landesdatennetz sowie von in IT-Systemen gespeicherten Daten mit Grundrechtsrelevanz (Fernmeldegeheimnis, informationelle Selbstbestimmung) unter Heranziehung von eingriffsmildernden Verfahrensvorkehrungen und Betroffenenrechten.
- **Zentraler Beauftragter für Informationssicherheit (CISO):** Gesetzliche Verankerung der Position des CISO im Hinblick auf Eingriffsbefugnisse zur Abwehr von Cybergefahren, sowie zu Berichtspflichten und zur Koordinierung des IT-Krisenmanagements.

II. Zu den Vorschriften im Einzelnen

1. § 2 Nr. 1 HITSiG-E – Begriffsbestimmungen

Ausweislich der Entwurfsbegründung basieren die herangezogenen Begriffsbestimmungen auf dem BSIG. Unklar ist, weshalb im Entwurf des HITSiG geringfügig von den entsprechenden BSI-Bestimmungen abgewichen wird, da dies einem einheitlichen systematischen Begriffsverständnis im deutschen IT-Sicherheitsrecht abträglich ist, ohne dass dafür ein sachlich nachvollziehbarer Grund bestehen würde. Datenschutzrechtlich ist die Übermittlung bzw. Übertragung überdies eine Form der Verarbeitung. Die Bestimmung sollte deshalb wie folgt formuliert werden: „Die Informationstechnik im Sinne dieses Gesetzes umfasst alle technischen Mittel zur Verarbeitung von Informationen“.

2. § 2 Nr. 2 HITSiG-E – Begriffsbestimmungen

Der Begriff der „Informationssicherheit“ als solcher wird im BSIG nicht definiert. Hier fehlt es gegenwärtig noch an einem klaren begrifflichen Verständnis des hessischen Regelungsvorschlags, da die Begriffe „IT-Sicherheit“, „Cybersicherheit“ und „Informationssicherheit“ eine unterschiedliche Bedeutung haben.[1] Da es im vorliegenden Gesetz wie in der Regelungsintention in Abschnitt I. dieser Stellungnahme um die Sicherheit von vernetzten IT-Systemen geht, wäre zumindest der Begriff der „IT-Sicherheit“ angemessener (die „Cybersicherheit“ findet sich bereits begrifflich nicht in der Gesetzesbezeichnung wieder wie es beispielsweise für Baden-Württemberg mit dem Cybersicherheitsgesetz in Anbetracht der skizzierten technischen Bedrohungslage treffender wäre). Überdies sollten die Schutzziele der IT-Sicherheit abschließend aufgeführt werden, mithin eine Ergänzung um Authentizität und Nichtabstreitbarkeit vorgenommen werden. Fraglich ist überdies, wie in der begrifflich engen Definition, die sich auf das IT-System und dessen Anwendung beschränkt, externe Dienste und Herausforderungen der digitalen Lieferkette angemessen Berücksichtigung finden sollen.

3. § 2 Nr. 3 HITSiG-E – Begriffsbestimmungen

Für die Definition der Schadprogramme wäre in Erweiterung der BSIG-Definition denkbar, zusätzlich den Begriff der Verarbeitung zu ergänzen, soweit dieser nicht unter die unbefugte „Nutzung“ und „Löschung“ von Daten fällt.

4. § 2 Nr. 4 HITSiG-E – Begriffsbestimmungen

Der rechtliche Begriff der „Sicherheitslücke“ ist spätestens seit den Entwicklungen zum Russland-Ukraine-Krieg im Jahr 2022 hoch politisiert und, wie von manch einem Autor behauptet wird, „verbrannt“. Dies ist vornehmlich auf einen juristisch bislang nicht korrigierten Auslegungsfehler des BSI bei der Anwen-

[1] Siehe zu den Begriffen im Einzelnen *Kipker*, Rechtshandbuch Cybersecurity, S. 2 f.

dung der Warnbestimmung zurückzuführen.[2] Wünschenswert wäre deshalb, die Begriffsbestimmung insoweit zu ergänzen bzw. umzuformulieren, sodass deutlich wird, dass es sich bei „Sicherheitslücken“ nicht um politisch zugängliche Wertungen, sondern um originär technisch-organisatorische und damit fachliche Beurteilungen handelt. Ansonsten führt dieser Begriff in der Folge zu einer erheblichen und im Praxisgebrauch weiter perpetuierten Rechtsunsicherheit, wie es aktuell bedauerlicherweise auch im BSIG der Fall ist.

5. § 3 HITSiG-E – Grundsätze der Informationssicherheit

Abs. 1 bestimmt grds. für die Stellen nach § 1 Nr. 1 und Nr. 2, dass angemessene organisatorische und technische Vorkehrungen sowie „sonstige Maßnahmen“ zur Gewährleistung der Informationssicherheit zu treffen sind. Was unter diesen „sonstigen Maßnahmen“ zu verstehen sein soll und inwieweit diese über die vorgeschlagenen TOM hinausgehen sollen, erschließt sich nicht. Empfohlen wird deshalb die Streichung dieser Ergänzung. Überdies wird wie folgt konkretisiert: „Für technische Maßnahmen soll der Stand der Technik maßgeblich sein“. Diese einengende Formulierung wird nicht empfohlen, auch findet sich keine Entsprechung in der bundesrechtlichen Bestimmung, in welcher der „Stand der Technik“ vielmehr auch die organisatorischen Maßnahmen einbezieht. Das erscheint an dieser Stelle sinnvoll, da der nachfolgende Verweis auf die IT-Grundschutzmethodik die Umsetzung eines ISMS verlangt, das eben nicht nur aus rein technischen Maßnahmen besteht. Auch „organisatorische Maßnahmen“ sind einer Bewertung nach dem Stand der Technik zugänglich, soweit sie im Kontext der IT-Sicherheit eingesetzt werden.

Abs. 3 bestimmt die Gewährleistungsverantwortung der Informationssicherheit für die jeweiligen Geschäftsbereiche. Vorgeschrieben wird die Benennung von ISBs. Hier sollte ergänzt werden, dass der ISB die erforderliche Qualifikation besitzen sollte, um die Aufgaben und Anforderungen seines Tätigkeitsbereichs angemessen zu erfüllen.

[2] Dazu im Detail *Kipker*, „Die Sicherheitslücke im BSIG – Möglichkeiten und Grenzen der juristischen Auslegung eines Rechtsbegriffs“, MMR 2023, 93 ff.

Abs. 4 legt fest, dass die ISBs an wesentlichen Änderungen von IT-Systemen zu beteiligen sind. Solche „wesentlichen Änderungen“ sollten spezifiziert werden, beispielsweise im Hinblick auf Funktionsauswirkungen, ihrem Bezugspunkt in der Hard- und Software oder mit Blick auf potenzielle Folgen für die Cybersicherheit. Unklar ist außerdem, welche Folge die Beteiligung des ISBs letztlich haben kann. Im Sinne der Informationssicherheit anzudenken wäre beispielsweise ein „Vetorecht“ des ISBs, falls bestimmte Änderungsvorschläge der IT-Infrastruktur grundlegende Sicherheitsbedenken zur Folge haben.

Für Abs. 5 wäre außerdem eine leichte begriffliche Verschärfung anzudenken, ohne damit die kommunale Selbstverwaltungsautonomie über Gebühr einzuschränken: Anstelle von „empfohlen“ die Formulierung „nahegelegt“.

6. § 4 HITSiG-E – Die oder der Zentrale Informationssicherheitsbeauftragte der Landesverwaltung

Der Zentrale Informationssicherheitsbeauftragte der Landesregierung ist für die Herstellung der ressortübergreifenden Informationssicherheit zuständig und nimmt in diesem Zusammenhang u.a. die Außenvertretung der hessischen Landesverwaltung in den Belangen der Informationssicherheit wahr. Die Aufgabenbeschreibung in Abs. 2 ist nicht abschließend, jedoch sollte hier noch stärker als in der bislang vorgeschlagenen Fassung der präventive Aspekt der Informationssicherheit, die Förderung von Cybersecurity Awareness und der Informationsaustausch als zentraler Stelle in den Mittelpunkt gestellt werden. Auch wäre es sinnvoll, die Abgrenzung zu weiteren IT-bezogenen Ämtern im Bereich der Landesverwaltung in Kürze zu skizzieren und begrifflich darzustellen. Im Hinblick auf die Befugnisse des CISO nach Abs. 3 ist die Anordnungsbefugnis zu IT-Sicherheitsmaßnahmen bei Gefahr im Verzug sinnvoll. Ergänzend wäre noch eine Begründungspflicht der Dienststellen im Allgemeinen anzudenken, sollten sie den Empfehlungen des CISO nicht folgen bzw. eigene Maßnahmen zur Cybersicherheit ergreifen.

7. § 5 HITSiG-E – Zentrum für Informationssicherheit

Das Zentrum für Informationssicherheit ist durch den für die IT- und Cybersicherheit in der Landesverwaltung zuständigen Minister einzurichten. Die Aufgaben sind vielfältig und betreffen in erster Linie eine aktive Koordinierungsfunktion sowie Aufgaben der Sammlung und Auswertung cybersicherheitsrelevanter Informationen. Insgesamt sollte dabei deutlich werden, dass das Zentrum für Informationssicherheit zuvorderst eine präventive Rolle für den Aufbau effektiver Informationssicherheitsinfrastrukturen darstellt, so werden in der Entwurfsfassung bislang keine Fragen des Informationssicherheitsmanagements begrifflich deutlich adressiert. Ebenso fehlen in der Aufgabenbeschreibung Vorgaben zur Zusammenarbeit mit privaten Stellen (insb. public private partnerships) zur Verbesserung der Effektivität nach dem HITSiG getroffener und zu treffender Maßnahmen. Hier sollte noch stärker als bislang die multidimensionale Bedrohungslage Berücksichtigung finden, da Bedrohungen für den privaten Sektor auch für den öffentlichen Sektor relevant sein können und eine Zusammenarbeit an dieser Stelle deshalb sinnvoll erscheint – dies insbesondere auch vor dem Hintergrund, dass Bestandteil des Zentrums für Informationssicherheit das CERT ist, das die Funktion als zentrale Kontaktstelle nach dem BSIG wahrnimmt und seine Leistungen auch gegenüber privaten Unternehmen erbringen kann.

8. § 6 HITSiG-E – Zentraler IT-Dienstleister des Landes

Die Hessische Zentrale für Datenverarbeitung (HZD) ist zentraler IT-Dienstleister für Informations- und Kommunikationstechnik für alle Behörden, Gerichte und sonstigen öffentlichen Stellen des Landes Hessen. Die HZD ist für den sicheren Betrieb für den Teil der IT-Infrastruktur der Landesverwaltung verantwortlich, den sie beeinflussen kann. Ein umfassender, dauerhafter und zügiger Informationsaustausch zwischen der HZD und dem Zentrum für Informationssicherheit ist deshalb essenziell für eine effektive Cybersecurity. Laut Gesetzeswortlaut ist dieser Informationsaustausch bislang vor allem einseitiger Natur und geht primär von der HZD in Richtung Zentrum für Informationssicherheit

und CISO. Hier sollte eine gesetzliche Informationsparität dergestalt hergestellt werden, als dass auch ein Informationsaustusch in Richtung der HZD möglich ist, indem explizit Anfragen an diese gestellt werden können. Unklar ist außerdem, weshalb die an sich wünschenswerte Vorgabe „Erkenntnisse im Zusammenhang mit der Informationssicherheit unverzüglich zu teilen“ nur Eingang in die Entwurfsbegründung, nicht aber in den eigentlichen Wortlaut der Vorschrift gefunden hat.

9. § 7 HITSiG-E – Datenverarbeitung

Systematisch ist im Hinblick auf diese Vorschrift generell anzumerken, dass ihre Rolle im Gesamtgefüge der Datenverarbeitungsvorschriften nicht klar definiert ist, da daneben auch weitere Datenverarbeitungstatbestände existieren, in deren Rahmen die Verarbeitung von personenbezogenen Daten nicht ausgeschlossen werden kann und die auch nicht klar als solche gekennzeichnet sind. Fraglich ist somit, welcher Tatbestand in welchen Fällen gilt. In jedem Falle handelt es sich bei § 7 aber um eine Vorschrift zur Verarbeitung von personenbezogenen Daten, sodass sich diese Angabe auch im Titel bzw. der Gesetzesbezeichnung wiederfinden sollte.

Abs. 1 bestimmt, dass das Zentrum für Informationssicherheit personenbezogene Daten zur Erfüllung seiner im öffentlichen Interesse liegenden Aufgaben verarbeiten darf. Dies sollte dergestalt konkretisiert werden, als dass zumindest ein Verweis auf die (abschließende) Aufgabenbeschreibung nach § 5 Abs. 2 HITSiG-E gegeben ist.

Die Ergebnisse der Interessenabwägung nach Abs. 2 sind zu dokumentieren.

Abs. 3 regelt die Anonymisierung der personenbezogenen Daten für eine Datenverarbeitung nach Abschluss des Auswertungsvorgangs. Da unterschiedliche Anonymisierungstechniken zur Verfügung stehen, sollte ergänzt werden, dass die Anonymisierung nach dem „Stand der Technik“ zu erfolgen hat. Im Übrigen entbindet eine Anonymisierung nicht vollständig von der datenschutzrechtlichen Verantwortlichkeit. Deshalb sollte die Vorschrift um einen zusätzlichen Passus

ergänzt werden, der eine regelmäßige Überprüfung des verwendeten Anonymisierungsverfahrens und alternativ eine Datenlöschung vorschreibt. Begrifflich sollte Abs. 3 S. 2 korrigiert werden, der irreführend von „anonymisierten personenbezogenen Daten“ spricht.

Abs. 4 bestimmt, dass, soweit es die Datenauswertungen ergeben, ein Schadprogramm identifiziert wurde, dieses jederzeit beseitigt werden kann oder in seiner Funktionsweise gehindert werden kann. Dies betrifft auch Fälle des § 303a StGB. Es mutet befremdlich an, dass sich eine derartige Befugnisgrundlage in einer Datenverarbeitungs- bzw. Datenschutzvorschrift befindet. Eine vergleichbare Regelung wurde im Cybersicherheitsgesetz Baden-Württemberg im Rahmen der Gefahrenabwehr für die Cybersicherheit getroffen. Ohnehin ist im Sinne der technischen IT-Sicherheit fraglich, ob die Vorschrift in dieser Weite formuliert wirklich sinnstiftend ist, da keinerlei Hinweise auf die Art der Gefahr, ihren Umfang und ihre Herkunft gegeben werden. Außerdem unklar ist, welche technischen Eingriffe in ein IT-System mit einer solchen „Beseitigung“ verbunden sein sollen.

10. § 8 HITSiG-E – Verwendung von auf informationstechnischen Systemen gespeicherten Daten

Grundsätzlich ist es im Sinne der Informationssicherheit sinnvoll, Protokolldaten bzw. Metadaten automatisiert zu verarbeiten. Eine entsprechende Rechtsgrundlage sollte deshalb im HITSiG vorgesehen werden. Dabei berücksichtigt werden muss jedoch auch, dass derartige Metadaten einen Personenbezug enthalten bzw. enthalten können (beispielsweise durch Kumulierung der Daten oder weil es sich um im konkreten Anwendungskontext einzigartige Daten handelt). Diese Eigenschaft berücksichtigt § 8 in der gegenwärtig vorliegenden Fassung nicht ausreichend, indem z.B. technisch-organisatorische Schutzvorkehrungen und Überprüfungen vorgeschlagen werden. Zwar enthält die systematisch nachfolgende Regelung des § 14 HITSiG-E Anforderungen an die Gewährleistung von Informationssicherheit und Datenschutz, hilfreich wäre hier jedoch schon an

dieser Stelle ein Verweis auf diese flankierende Verfahrensvorschrift. In dem vorgenannten Zusammenhang ist deshalb auch das systematische Verhältnis zu § 7 HITSiG-E unklar.

Eine vergleichbare Problematik haftet der Vorschrift § 9 HITSiG-E (Erhebung und Auswertung des Datenverkehrs im Landesdatennetz) an, da die Regelungen inhaltlich ähnlich ausgestaltet sind.

11. § 10 HITSiG-E – Auswertung ohne Inhaltsdaten

§ 10 HITSiG-E stellt eine flankierende Vorschrift zur Datenauswertung zu Zwecken der Informationssicherheit (ohne Inhaltsdaten) gem. §§ 8 und 9 HITSiG-E dar, die offensichtlich wie dargestellt von einem Personenbezug der in diesem Kontext verarbeiteten Daten ausgeht. Dies sollte deshalb begrifflich nicht nur in § 10, sondern auch schon in den §§ 8 und 9 des Gesetzes deutlich werden.
Im Sinne des Datenschutzes hingegen positiv hervorzuheben ist der Fokus auf der automatisierten Auswertung der Daten, um die Intensität eines eventuellen Grundrechtseingriffs gemäß den bundesverfassungsrechtlichen Vorgaben zu reduzieren. Für eine manuelle oder personenbezogene Datenauswertung werden Einschränkungstatbestände formuliert. Fraglich ist in diesem Zusammenhang, welche weiteren Verarbeitungsvorgänge über Abs. 1 hinausgehend relevant sein sollen, wie die Formulierung „insbesondere“ nahelegt. Zwar formuliert Abs. 2 einschränkende Anforderungen für die über Abs. 1 hinausgehende Datenverarbeitung, die aber nicht ausreichend sind, da sie – eben weil es sich um personenbezogene Daten handelt – die verfassungsrechtlich geschützten Rechtspositionen des durch die Datenverarbeitung Betroffenen nicht angemessen berücksichtigen, so beispielsweise im Zuge einer kumulativen Interessenabwägung der widerstreitenden Rechtsgüter. Allein die eingeschränkte Anordnungsbefugnis der Auswertungsmaßnahmen vermag dieses datenschutzrechtliche Defizit nicht auszugleichen.

12. § 11 HITSiG-E – Auswertung von Inhaltsdaten

§ 11 befasst sich im Kern mit der Auswertung von Inhaltsdaten. Auch diese Vorschrift leidet jedoch an den systematischen Mängeln des Datenschutz- bzw. Maßnahmenteils des HITSiG-E. Unklarerweise wird in Abs. 1 zunächst – obwohl es laut Titel bzw. Bezeichnung um eine Auswertung von Inhaltsdaten gehen soll, wieder auf die Auswertung von Metadaten nach §§ 8 und 9 abgestellt, wobei sich inhaltliche Überschneidungen insbesondere zu § 8 ergeben. Nicht deutlich wird dabei die Abgrenzung zwischen den nach den jeweiligen Vorschriften möglichen Maßnahmen, so z.B. auch für die unverzügliche Löschpflicht, die inhaltsgleich bereits in § 8 Abs. 2 S. 2 HITSiG-E geregelt ist. Auch für Abs. 3 fehlt es an einer dokumentierten Abwägung der widerstreitenden Interessen.

Im Übrigen ergibt sich aus Abs. 1-3 nicht, worin die Unterscheidung zwischen Verkehrs- und Inhaltsdaten liegen soll, wie die Bezeichnung der Vorschrift eigentlich erwarten lassen sollte.

Unvermittelt trifft Abs. 4 eine – juristisch zwar erforderliche – Regelung zum Kernbereichsschutz, ohne dass jedoch überhaupt deutlich wird, was unter Inhaltsdaten im Sinne des Gesetzes zu verstehen sein soll und aus welcher Quelle diese stammen.

13. § 14 HITSiG-E – Gewährleistung der Informationssicherheit und des Datenschutzes

Auch eine gesetzliche Vorschrift, die die Informationssicherheit befördern will, muss den Datenschutz und die Vorgaben an die Datensicherheit beachten, soweit sie zu diesem Zweck (personenbezogene) Daten auswertet. Deshalb ist zu begrüßen, dass die gegenwärtige Entwurfsfassung eine ausdrückliche Regelung hierzu beinhaltet. Gleichwohl wäre zur Klarstellung schon ein Verweis aus den vorangehenden und bezugnehmenden Vorschriften heraus auf § 14 HITSiG sinnvoll. Wie bereits im Rahmen der Begriffsbestimmungen angemerkt, sollte für Abs. 2 Nr. 4 erwogen werden, weitere Schutzziele der IT-Sicherheit zu ergänzen, da gerade im Rahmen einer verlässlichen Datenauswertung die Authentizität

und Nichtabstreitbarkeit unerlässlich sind. Lobenswert ist die ausdrückliche Verankerung des Vier-Augen-Prinzips beim Datenzugriff, die Anordnung der getrennten Datenhaltung sowie die Protokollierung der entsprechenden Datenverarbeitung inklusive eines Berechtigungsmanagements. Ebenso positiv hervorzuheben ist die Erstellung eines Sicherheitskonzepts gem. § 15 HITSiG-E – in dem Zusammenhang ist anzumerken, dass wesentliche Veränderungen der IT-Systeme auch die ihrer Nutzung zugrundeliegende Software betreffen können.

14. § 16 HITSiG-E – Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen der Beeinträchtigung

Abs. 4 enthält einen redaktionellen Fehler, richtig müsste es heißen: „[…] nur mit Einwilligung der ersuchenden Stelle nach Abs. 1 übermitteln […]“.

Abs. 5 regelt die Einbeziehung Dritter in die Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme. Dabei werden jedoch keinerlei weitere Anforderungen an die Dritten selbst, deren Befähigung und das Rechtsverhältnis zueinander festgelegt.

15. § 17 HITSiG-E – Information der Betroffenen

Die datenschutzrechtlichen und systematischen Unzulänglichkeiten des vorliegenden Gesetzentwurfs setzen sich bei der Information der Betroffenen als wichtiger verfassungsrechtlicher Gewährleistung fort (gerade auch im Hinblick auf das Zitiergebot als Beleg für den Grundrechtseingriff). Weshalb eine Betroffeneninformation nur in den Fällen des § 10 Abs. 2 oder des § 11 Abs. 3 einschlägig sein soll, wird nicht weiter ausgeführt. Dies ist rechtlich problematisch, denn es können – wie bereits angeführt wurde – auch im Kontext der anderen Verarbeitungsszenarien zur IT-Sicherheit nach diesem Gesetz personenbezogene Daten anfallen, die behördlich verarbeitet werden.

Universität Bremen

IGMR
Institut für Informations-,
Gesundheits- und Medizinrecht

Bremen, den 26. April 2023

Prof. Dr. jur. Dennis-Kenji Kipker